.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... 35

.....

.....

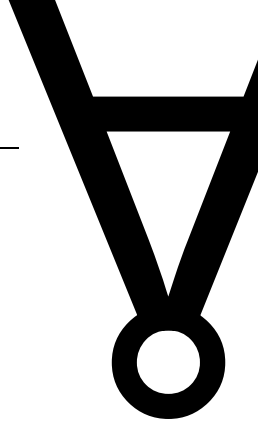
.....

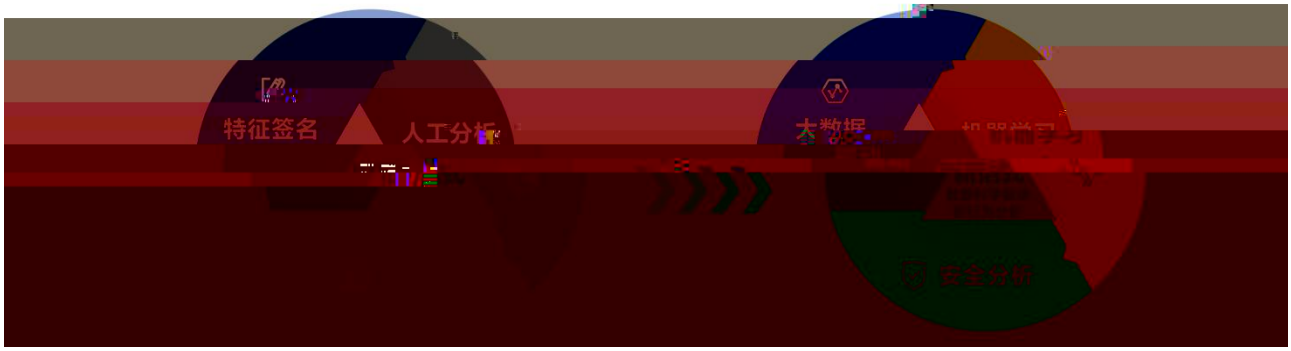
.....

.....

.....

1





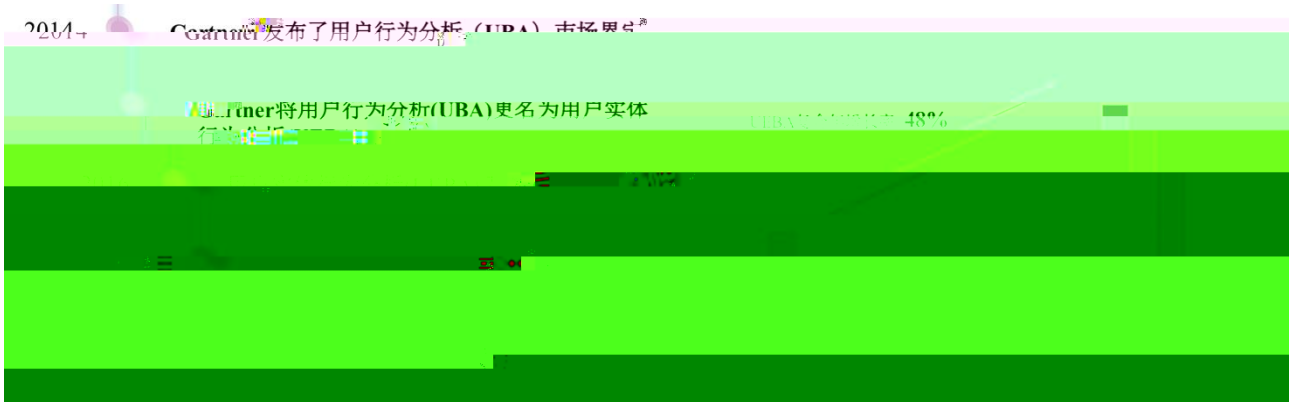
2

1.

2.

3.

4.



4 UEBA

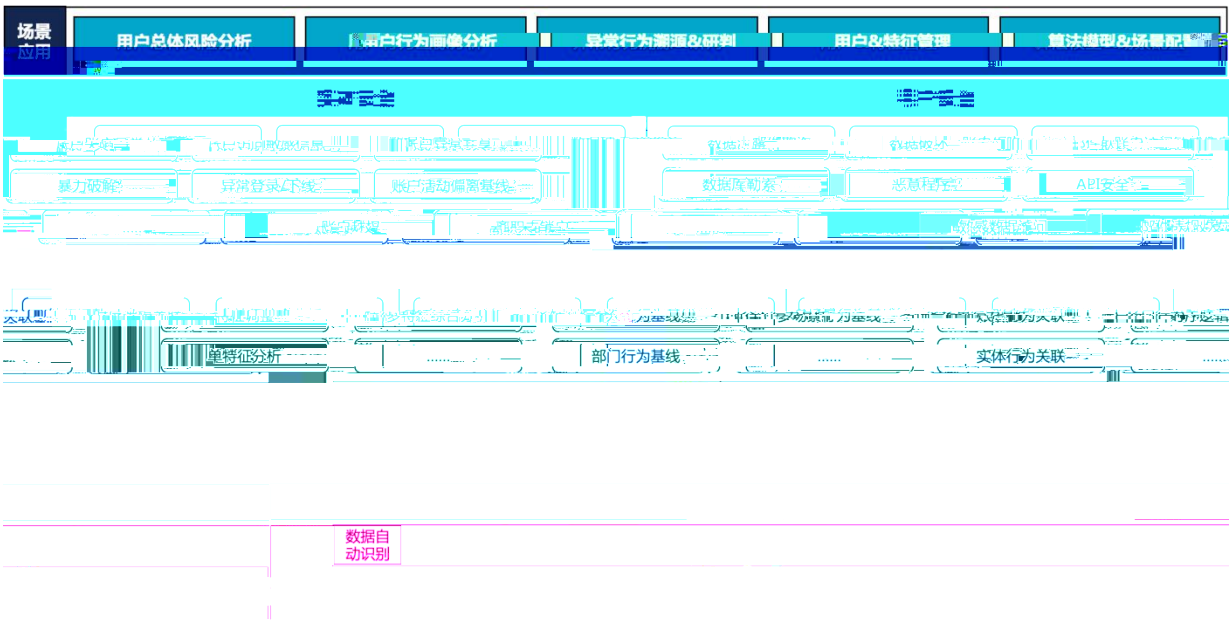
2

	UEBA/	IDS/AV/WAF	TI/

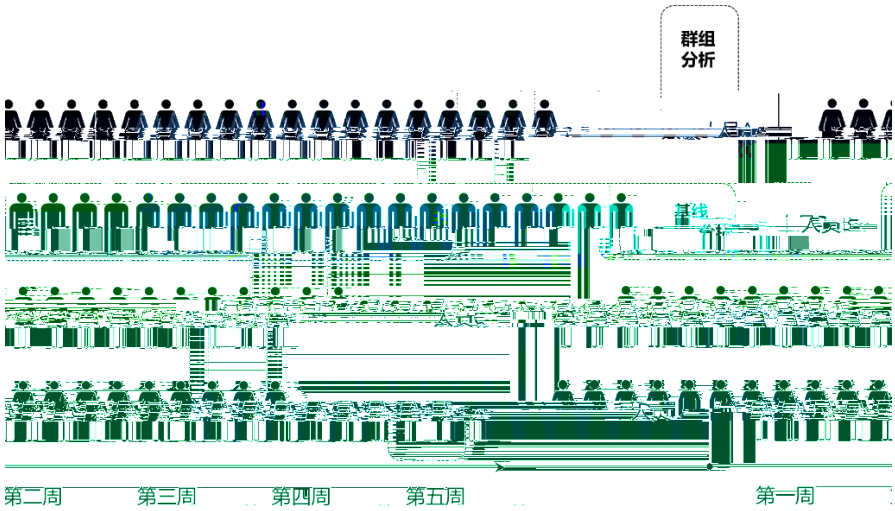
1.

2.

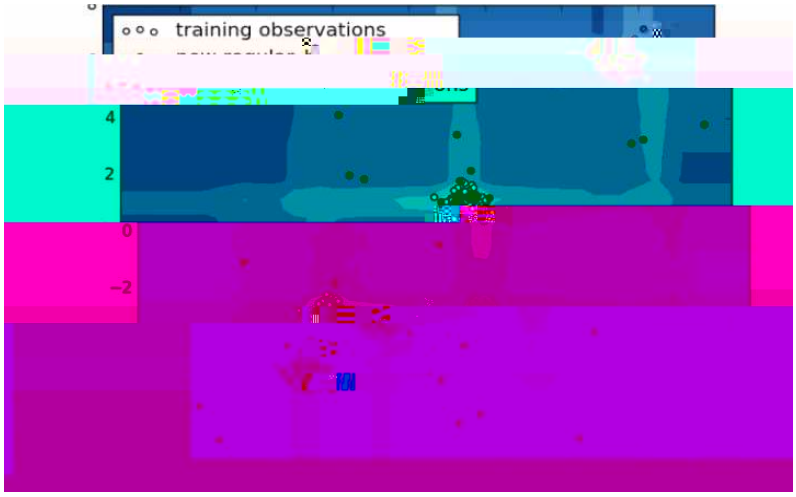
UE


场景应用
用户总体风险分析
用户行为画像分析
异常行为溯源&研判
用户&特征管理
暴力破解
异常登录/下线
账户活动偏离基线
数据库初查
恶意程序
API安全
单特征分析
部门行为基线
实体行为关联
数据自动识别

5 UEBA



6

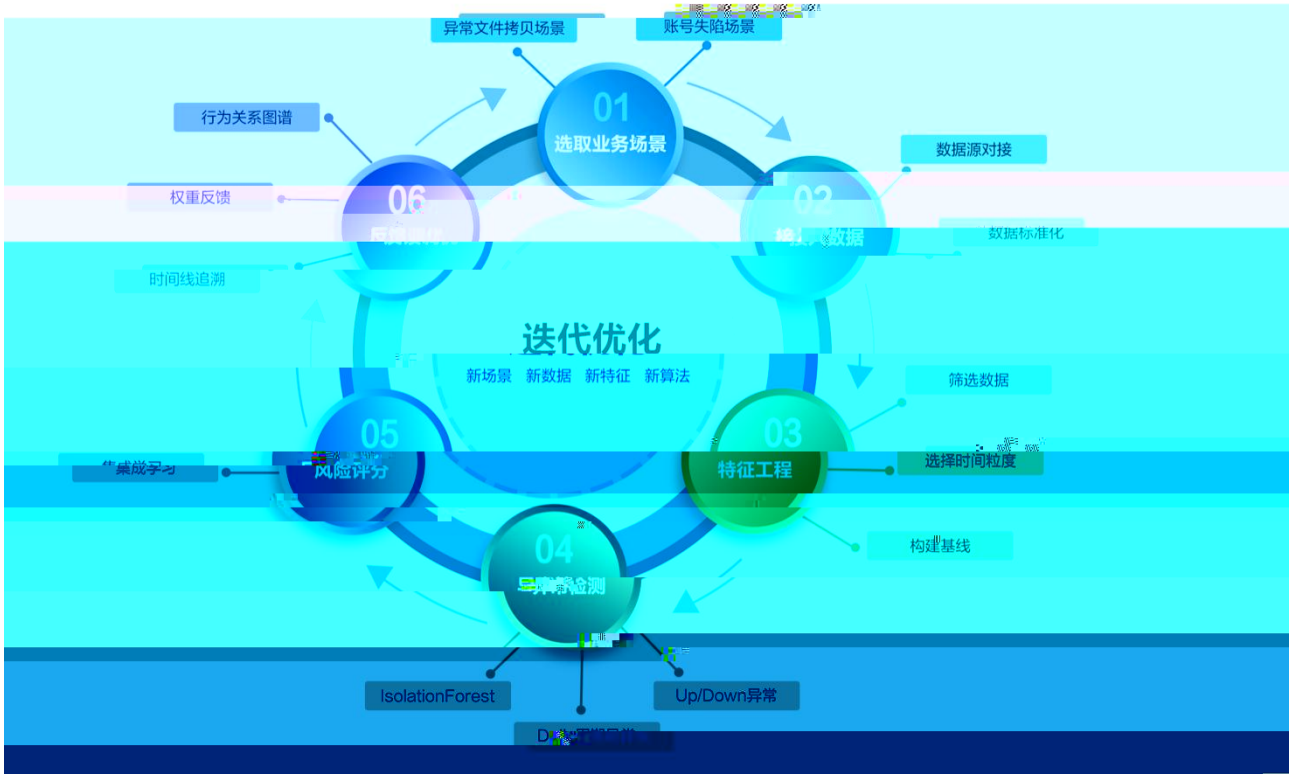


7

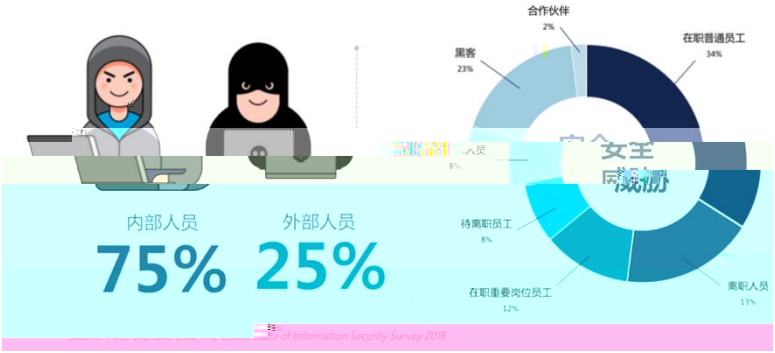


9

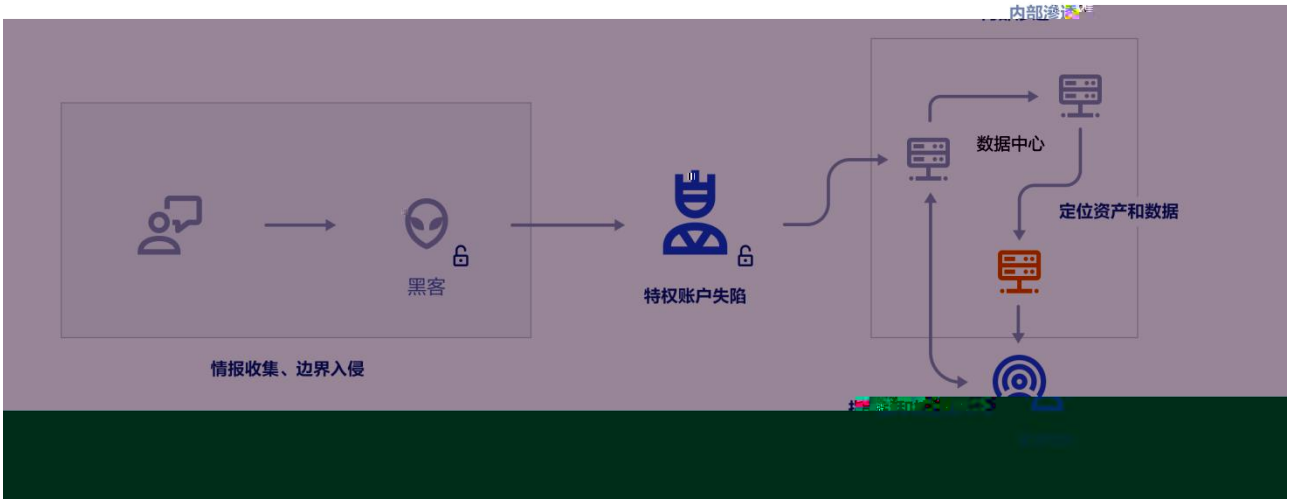
3.


异常文件拷贝场景
账号失陷场景
01
选取业务场景
行为关系图谱
数据源对接
权重反馈
06
02
数据标准化
时间线追溯
迭代优化
新场景 新数据 新特征 新算法
筛选数据
05
风险评分
03
特征工程
选择时间粒度
构建基线
04
IsolationForest
Up/Down异常

11 UEBA


内部人员
75%
外部人员
25%
合作伙伴
2%
在职普通员工
34%
黑客
23%
待离职员工
8%
在职重要岗位员工
12%
离职人员
13%


构建行为基线，
提取到了账户作息时间的异常行为信息。
基于疑问行为，
还原日志信息，


黑客
情报收集、边界入侵
特权账户失陷
数据中心
定位资产和数据


黑客
高级逃逸技术
病毒扩散
勒索病毒
挖矿
僵尸主机
网络
恶意软件

API

AiLPHA

